Quantum Key Distribution using Two Coherent States of Light and their Superposition

Yoshihiro Nambu, Akihisa Tomita, Yoshie Chiba-Kohno, and Kazuo Nakamura

Fundamental Research Laboratories, NEC Corporation,

34 Miyukigaoka, Tsukuba, Ibaraki 305-8501, Japan

(November 10, 1999)

Abstract

We describe a quantum key-distribution scheme in which two nearly orthogonal coherent states carry the key, and the superposition of these states (cat states) protects the communication channel from eavesdropping. Any eavesdropping activity can be detected from the disappearance of the interferential fringes in the distribution of the outcome when a certain quadrature component is measured through homodyne detection. This scheme is secure against conclusive-measurement attack and generalized beamsplitter attack, both believed to be a potential risk when multi-photon states are used as a quantum signal.

23.23.+x, 56.65.Dy

I. INTRODUCTION

The quantum key distribution (QKD) protocol provides a way for two remote parties (traditionally known as Alice and Bob) to share a secure random cryptographic key by communicating over an open channel [1–5]. Alice and Bob publicly communicate over a quantum channel and then exchange messages over a classical channel that can be monitored but not tampered with by an eavesdropper (Eve). Quantum mechanical complementarity ensures that any activities of potential eavesdroppers can be detected. Even if some eavesdropping is found, Alice and Bob can further process the obtained key (the raw key) to extract a safe but much shorter cryptographic key (the final key) by using a classical method of error correction (a reconciling protocol) and private amplification [6,7]. A secure message of equal length to the final key can be transmitted over the classical channel by conventional encryption methods such as the one-time pad method [8]. The security of the encrypted communication depends directly on the security of the final key.

Among the protocols proposed so far, the four-state scheme, usually referred to as the BB84 protocol [2], is claimed to be provably secure under the assumption that Alice uses a perfect single-photon source [9]. In this protocol, Alice and Bob use two conjugate bases (say, a rectilinear basis, $+$, and a diagonal basis, $\times$) for the polarization of a single photon. In basis $+$, they use two orthogonal states $|0_+\rangle$ and $|1_+\rangle$ to encode logical "0" and "1", respectively, and in basis $\times$, $|0_\times\rangle$ $(= \left(1/\sqrt{2}\right)[|0_+\rangle + |1_+\rangle])$ and $|1_\times\rangle$ $(= \left(1/\sqrt{2}\right)[|0_+\rangle - |1_+\rangle])$. Alice transmits a random sequence of these states through their quantum channel and Bob measures each state with a basis randomly chosen from $\{+, \times\}$. After transmission, the basis is revealed, which enables Bob to discard the data that Alice and Bob used a different basis to encode and decode and that provide inconclusive results to Bob. The remaining data, which is called the sifted key [10], should agree for Alice and Bob and yield conclusive results for Bob.

The key idea of the BB84 protocol is that simultaneous measurements of non-commuting observables for a single quanta are forbidden by quantum mechanics. For these non-commuting observables, the measurement of one observable made on the eigenstate of another observable inevitably introduces disturbance to the state because of the back reaction of the measurement. Since Eve has no *a priori* information about the randomly chosen bases of each bit in the sifted key, she is forced to guess which observable to measure for each photon. On average, half the time Eve will guess wrong and thus introduce a disturbance into the state. The disturbance can be detected as a bit error by comparing parts of the sifted key.

The theoretical QKD schemes that have been proven secure against a wide class of attacks have involved the transmission of a single quantum particle that is subject to quantum mechanical complementarity. On the other hand, there has been growing interest among researchers on quantum information processing using multi-photon states [11,12]. Several authors have extended this idea and have recently proposed a QKD scheme that uses multi-photon states as a quantum carrier [13–15]. All these authors used squeezed states, in which the key data are encoded on continuous, conjugate observables of the field quadrature components. Hillery further suggested that any nonlocal field state is useful for quantum information processing and communication [14]. In this paper, we provide another example that supports this suggestion by showing that the secure BB84 protocol can be constructed by using two nearly orthogonal coherent states and the superposition of these states (cat states).

The organization of this paper is as follows. Section II reviews the BB84 protocol. The connection between the protocol and the information exclusion principle proposed by Hall [16] is discussed and a comprehensive explanation of the principle of the BB84 protocol is given. Section III is devoted to the main subject of this paper. The basic idea and the protocol of the QKD scheme using two coherent states and their superposed state are presented, and the principle and security of this scheme are discussed. In Sec. IV, we summarize the main results of the paper.

II. BB84 PROTOCOL

The BB84 protocol can most clearly be understood in terms of the information exclusion principle [16]. The information exclusion principle provides an information-theoretic description of quantum complementarity and imposes an upper bound on the sum of the information gain obtained from observation of complementary observables in a quantum ensemble. Consider two observables A and B of a quantum system with an N-dimensional Hilbert space. They are said to be complementary if their eigenvalues are nondegenerate, and the overlap of any two normalized eigenvectors $|a_j\rangle$ of A and $|b_j\rangle$ of B satisfy $|\langle a_i|b_j\rangle| = 1/\sqrt{N}$; therefore, the eigenstates of A are equally weighted superpositions of the eigenstates of B, and vice versa. Thus, when the system is in an eigenstate of A, all possible outcomes of a measurement of B are equally probable; i.e., precise knowledge of the measured value of one observable implies maximal uncertainty of the measured value of the other. In such a case, an operator B is the generator of shifts in the eigenvalue of any eigenstate of A; $\exp(iBl)\,|a_j\rangle = \left|a_{(j+l)\,\mathrm{mod}\,N}\right\rangle$, and vice versa, $\exp(iAm)\,|b_j\rangle = \left|b_{(j-m)\,\mathrm{mod}\,N}\right\rangle$ [17]. Let ρ be a state of an given ensemble which is prepared with *a priori* probability p_i in the known state ρ_i, so $\rho = \sum_i p_i \rho_i$. The initial entropy of the system is $H_{int} = H(\rho) = -\sum_i p_i \log_2 p_i$ (in bits). Given the conditional probability $P(a_j|\rho_i) = tr(\rho_i A_j)$ for obtaining outcome a_j when measuring an observable A when the state is prepared in ρ_i, where $A_j = |a_j\rangle\langle a_j|$, we can compute the *a posteriori* probability $Q(\rho_i|a_j)$ for preparation ρ_i by Bayes's theorem as $Q(\rho_i|a_j) = P(a_j|\rho_i)p_i/q_j$, where $q_j = \sum_i P(a_j|\rho_i)p_i$ is the *a priori* probability for the occurence of outcome a_j. After the measurement, the average entropy (in bits) becomes $H_{fin} = H(\rho|A) = -\sum_j q_j \sum_i Q(\rho_i|a_j)\log_2 Q(\rho_i|a_j)$. The average information gain (in bits) is $I(\rho;A) \equiv H_{ini} - H_{fin} = H(\rho) - H(\rho|A) = -\sum_i p_i \log_2 p_i + \sum_j q_j \sum_i Q(\rho_i|a_j)\log_2 Q(\rho_i|a_j)$ [18,19]. Hall proved that the inequality

$$I\left(\rho;A\right) + I\left(\rho;B\right) \leq 2\log_2 N\xi = \log_2 N \tag{2.1}$$

holds for Shannon mutual information for the measurement of complementary observables A and B on a system in arbitrary state ρ, where $\xi = \max|\langle a_j|b_j\rangle| = 1/\sqrt{N}$ [16]. When $N = 2$, inequality (2.1) means that the recoverable information can never exceed the maximal von Neumann entropy ($S_{\max} = 1$) bit of the system, which depends only on the dimension – the number of distinguishable pure states – of the Hilbert space in which the signal states lie. Inequality (2.1) states that the information gain corresponding to the measurement of an observable can be maximized only at the expense of the information gains corresponding to the measurement of the complementary observable. Hall named inequality (2.1) the information exclusion principle and showed that it is closely related to Heisenberg's uncertainty principle and Bohr's complementary principle [16].

To see how the information exclusion principle relates to the BB84 protocol, let us briefly review the optimal eavesdropping strategy within an individual-attack scheme in which each signal carrier sent by Alice is independently subject to eavesdropping. In this strategy, Eve lets a probe of arbitrary dimensions interact with each signal carrier independently. As a result, each of her probes is correlated to a transmitted state and its partial information is imprinted onto the probe. She then delays her measurement and keeps the quantum information in her probes until she learns the bases used by Alice and Bob from their public announcement. She finally tries to extract as much information as possible about the transmitted states by measuring her probes. To avoid revealing herself in too straightforward a manner by introducing different error rates in the different bases (because the error rate should be independent of the basis if the errors are due to a random process), Eve applies a symmetric eavesdropping strategy that treats the two bases on an equal footing. This strategy has been shown to require a two-qubit probe – i.e., a quantum system with a four-dimensional Hilbert space – and to be optimal by Fuchs [20]. He proved that the joint unitary operation U acting on the Hilbert space of the carrier and probe is a state-dependent optimal quantum-cloning process [21–23] that is given by

$$\begin{aligned} |\psi\rangle\,|0_x\rangle &\rightarrow U\,|\psi\rangle\,|0_x\rangle \\ &= \sqrt{F}\left|\tilde{\psi}^x_{00}\right\rangle|0_x\rangle + \sqrt{D}\left|\tilde{\psi}^x_{01}\right\rangle|1_x\rangle\,, \qquad (2.2) \\ |\psi\rangle\,|1_x\rangle &\rightarrow U\,|\psi\rangle\,|1_x\rangle \end{aligned}$$

$$= \sqrt{D} \left| \tilde{\psi}_{10}^{x} \right\rangle |0_x\rangle + \sqrt{F} \left| \tilde{\psi}_{11}^{x} \right\rangle |1_x\rangle , \tag{2.3}$$

$$\left| \tilde{\psi}_{mn}^{x} \right\rangle \equiv \langle m_x | U |\psi\rangle |n_x\rangle / |\langle m_x | U |\psi\rangle |n_x\rangle| , \tag{2.4}$$

for $x = +, \times$ and $m, n = 0, 1$, where $F + D = 1$, and $|\psi\rangle$ is the initial state of each of Eve's probes and $\left| \tilde{\psi}_{mn}^{x} \right\rangle$ is its normalized state after interaction. The four possible states of $\left| \tilde{\psi}_{mn}^{x} \right\rangle$ are not necessarily orthogonal to each other, but all scalar products other than $\left\langle \tilde{\psi}_{11}^{x} | \tilde{\psi}_{00}^{x} \right\rangle = \left\langle \tilde{\psi}_{00}^{x} | \tilde{\psi}_{11}^{x} \right\rangle = \left\langle \tilde{\psi}_{10}^{x} | \tilde{\psi}_{01}^{x} \right\rangle = \left\langle \tilde{\psi}_{01}^{x} | \tilde{\psi}_{10}^{x} \right\rangle \equiv \mathcal{V}$ must be zero and $\mathcal{V}$ must equal $F - D$ in order to symmetrize the strategy [24].

Let us calculate the probabilities that Bob and Eve will correctly infer the state transmitted by Alice when Eve uses this eavesdropping strategy. These probabilities are characterized by the conditional probability $P(j|i)$ of obtaining outcome j, given that state ρ_i was transmitted by Alice. Suppose that Alice transmits either $\rho_{0x} = |0_x\rangle \langle 0_x|$ or $\rho_{1x} = |1_x\rangle \langle 1_x|$. Bob's marginal density matrices ρ_{ix}^{B}, and Eve's, ρ_{ix}^{E}, after the signal-probe interaction and without learning each other's measurement outcomes (nonselective measurement), are easily calculated as

$$\begin{aligned}
\rho_{0x}^{B} &= \mathcal{E}^{B}(\rho_{0x}) = tr_E U |\psi\rangle \langle\psi| \otimes \rho_{0x} U^{-1} \\
&= F\rho_{0x} + D\rho_{1x}, \qquad (2.5) \\
\rho_{1x}^{B} &= \mathcal{E}^{B}(\rho_{1x}) = tr_E U |\psi\rangle \langle\psi| \otimes \rho_{1x} U^{-1} \\
&= D\rho_{0x} + F\rho_{1x}, \qquad (2.6) \\
\rho_{0x}^{E} &= \mathcal{E}^{E}(\rho_{0x}) = tr_B U |\psi\rangle \langle\psi| \otimes \rho_{0x} U^{-1} \\
&= F\sigma_{00}^{x} + D\sigma_{01}^{x}, \qquad (2.7) \\
\rho_{1x}^{E} &= \mathcal{E}^{E}(\rho_{1x}) = tr_B U |\psi\rangle \langle\psi| \otimes \rho_{1x} U^{-1} \\
&= D\sigma_{10}^{x} + F\sigma_{11}^{x}, \qquad (2.8)
\end{aligned}$$

where $\sigma_{mn}^{x} = \left| \tilde{\psi}_{mn}^{x} \right\rangle \left\langle \tilde{\psi}_{mn}^{x} \right|$ and $\mathcal{E}(\rho)$ is a trace-preserving, completely positive, linear map of the density operators of Alice, and Eqs. (2.5)-(2.8) define the unitary representation [25–27] of the map. When Bob performs a standard measurement on the sifted key, the conditional probabilities of Bob's inference of his signal j when Alice sends signal i are, for $x = +, \times$ and $i, j = 0, 1$,

$$P_x^{AB}(j|i) = tr\left(\rho_{ix}^B \left|j_x\right\rangle \left\langle j_x\right|\right) = \begin{cases} F = \frac{1+\mathcal{V}}{2} & \text{if } i = j \\ D = \frac{1-\mathcal{V}}{2} & \text{if } i \neq j \end{cases}. \tag{2.9}$$

On the other hand, Eve's strategy is first to distinguish between two mutually orthogonal sets $S_i = \{\sigma_{i0}^x, \sigma_{i1}^x\}$ $(i = 0, 1)$ that can be perfectly separated with a standard measurement. She next performs a measurement that distinguishes between σ_{00}^x and σ_{11}^x or between σ_{01}^x and σ_{10}^x, which are not necessary mutually orthogonal ($tr\sigma_{00}^x\sigma_{11}^x = tr\sigma_{01}^x\sigma_{10}^x \neq 0$), that gives the smallest possible error probability. This is the best she can do in terms of the information gained from the sifted key [24]. It is well known that such a measurement is realized by standard measurement in the basis in the Hilbert space spanned by $\left|\tilde{\psi}_{00}^x\right\rangle$ and $\left|\tilde{\psi}_{11}^x\right\rangle$ or by $\left|\tilde{\psi}_{01}^x\right\rangle$ and $\left|\tilde{\psi}_{10}^x\right\rangle$ that straddles these vectors [28–32]. This measurement gives the conditional probabilities of Eve's inference of her signal j when Alice sends signal i as

$$P_x^{AE}(j|i) = tr\left(\rho_{ix}^E \widehat{\Pi}_j^x\right) = \begin{cases} \frac{1}{2}\left(1 + \mathcal{D}_{opt}\right) = \frac{1+\sqrt{1-\mathcal{V}^2}}{2} & \text{if } i = j \\ \frac{1}{2}\left(1 - \mathcal{D}_{opt}\right) = \frac{1-\sqrt{1-\mathcal{V}^2}}{2} & \text{if } i \neq j \end{cases}, \tag{2.10}$$

where $\mathcal{D}_{opt} = tr\left|\sigma_{00}^x - \sigma_{11}^x\right| = tr\left|\sigma_{01}^x - \sigma_{10}^x\right| = \sqrt{1-\mathcal{V}^2}$ is the distance between σ_{00}^x and σ_{11}^x and between σ_{01}^x and σ_{10}^x in the trace-class norm, and $\widehat{\Pi}_0^x$ and $\widehat{\Pi}_1^x$ are the projection-valued measures (PVMs) corresponding to the above detection strategy to distinguishe between ρ_{0x}^E and ρ_{1x}^E. (Eve also knows when Bob has received an error) [20,32–35]. Finally, upon assuming equal *a priori* probabilities $p_{0+} = p_{1+} = p_{0\times} = p_{1\times}$, Bob's average probability (*a posteriori* probability) of correct (incorrect) inference of the state transmitted by Alice, Q_c^B (Q_e^B), is given by $\frac{1}{2}\left(P_+^{AB}(j|i) + P_\times^{AB}(j|i)\right)$ with $i = j$ $(i \neq j)$ and Eve's average probability, Q_c^E (Q_e^E), is given by $\frac{1}{2}\left(P_+^{AE}(j|i) + P_\times^{AE}(j|i)\right)$ with $i = j$ $(i \neq j)$. Thus, $Q_c^B = \frac{1+\mathcal{V}}{2}$ and $Q_c^E = \frac{1+\sqrt{1-\mathcal{V}^2}}{2}$ gives Bob's and Eve's fidelity, respectively, and $Q_e^B = \frac{1-\mathcal{V}}{2}$ and $Q_e^E = \frac{1-\sqrt{1-\mathcal{V}^2}}{2}$ gives Bob's and Eve's error probability, respectively. $G^B = Q_c^B - Q_e^B = \mathcal{V}$ and $G^E = Q_c^E - Q_e^E = \mathcal{D}_{opt}$ are convenient measures of Bob's and Eve's information gain [20]. Since these measures satisfy $\left(G^B\right)^2 + \left(G^E\right)^2 = \mathcal{D}_{opt}^2 + \mathcal{V}^2 = 1$, there is a trade-off relation between Bob's and Eve's information gain.

From an information-theoretic point of view, the mutual information I_{AB} between Alice and Bob and I_{AE} between Alice and Eve concerning Alice's message is more appropriate for evaluating Bob's and Eve's knowledge about the sifted key. Mutual information is the measure of information successfully transmitted from input to output. Since Alice and Bob, in general, cannot distinguish between errors caused by an eavesdropper and errors caused by the environment, they have to assume that all errors are due to a potential eavesdropper. As long as Bob's error rate, Q_e^B, is small, the errors can be accepted and corrected by legitimate users. As a result, Eve can obtain some information about the transmitted data. If the noise in the channel is such that $I_{AB} < I_{AE}$ for any potential eavesdropper, then Alice and Bob should consider the transmission channel to be unsafe. On the contrary, if $I_{AB} > I_{AE}$, they may still be able to extract a safe but much shorter cryptographic key by means of error correction and private amplification [6,7]. Moreover, in a classical context there is, at least in principle, a way for Alice and Bob to exploit any positive difference, $I_{AB} - I_{AE}$, to create a reliably secret string of key bits that has a length of about $I_{AB} - I_{AE}$ [36–38]. It is therefore important to estimate the maximal amount of information available to Bob and Eve for a given error rate Q_e^B that Bob can evaluate. With equiprobable signals, the average information gain is given by $I_{AB} = 1 - H(Q_e^B)$ and $I_{AE} = 1 - H(Q_e^E)$, where $H(q) = -q \log_2 q - (1-q)\log_2(1-q)$ is the entropy function (in bits) and is a nonlinear function of q. The upper plot in Fig. 1 shows I_{AB}, I_{AE} and $I_{AB} + I_{AE}$ plotted against Q_e^B, and the lower plot shows G^B and G^E. From this figure, it is clear that there is a trade-off relation between I_{AB} and I_{AE} as well as a trade-off relation between G^B and G^E. The sum $I_{AB} + I_{AE}$ never exceeds unity ($I_{AB} + I_{AE} \leq 1$); that is, the sum can never exceed the maximal amount of information that can be encoded in a two-level system. This condition must be met for the BB84 protocol to work. Therefore, we can see that Eve's acquired information I_{AE} is bounded by $1 - I_{AB}$ which Alice and Bob can easily evaluate from the bit error rate in Bob's data.

The last inequality, $I_{AB}+I_{AE} \leq 1$, is closely related to the information exclusion principle. This is because the above eavesdropping strategy can be alternatively viewed as a method for simultaneously measuring non-commuting observables. To see this, consider the unitary operation in Eqs. (2.2) and (2.3) with $x = +$, $F = 1$, and $D = 0$. This operation is called measurement of intensity γ, where $\left\langle \tilde{\psi}_{11}^{+} | \tilde{\psi}_{00}^{+} \right\rangle = \left\langle \tilde{\psi}_{00}^{+} | \tilde{\psi}_{11}^{+} \right\rangle = \cos\gamma = \mathcal{V}$. [23] When Alice and Bob have chosen the basis $+$, Eve causes no disturbance and obtains information about the bit to the extent that she can distinguish the two vectors $\left| \tilde{\psi}_{00}^{+} \right\rangle$ and $\left| \tilde{\psi}_{11}^{+} \right\rangle$, whose error probability is $\frac{1-\sqrt{1-\mathcal{V}^2}}{2}$. Conversely, if Alice and Bob have chosen the basis $\times$, Eve learns nothing and introduces an error with probability $\frac{1-\mathcal{V}}{2}$. Bob's and Eve's information gains when Alice transmits bits with the $+$ basis are therefore $I_{AB}^{+} = 1$ and $I_{AE}^{+} = 1 - H(\frac{1-\sqrt{1-\mathcal{V}^2}}{2})$, and their information gains when Alice transmits the bits with the $\times$ basis are $I_{AB}^{\times} = 1 - H(\frac{1-\mathcal{V}}{2})$ and $I_{AE}^{\times} = 0$. Thus, this operation is clearly asymmetric with respect to the basis used in which Eve obtains information on the bits sent with one basis at the cost of a disturbance in the bits sent with the other basis. In this operation, Eve obtains information only about the observable $P_{+}(= |i_{+}\rangle \langle i_{+}|)$ of the $+$ basis on the system, while Bob obtains information about both P_{+} and $P_{\times}(= |i_{\times}\rangle \langle i_{\times}|)$ of the $\times$ basis. Thus, when Bob observes $P_{\times}$, the above operation provides a method for simultaneously measuring complementary observables, P_{+} and $P_{\times}$ in which the outcome for Eve gives the information $I_{AE} = I(\rho; P_{+})$ and that for Bob gives $I_{AB} = I(\rho; P_{\times})$.

When we extend this argument to the symmetric operation associated with an optimal eavesdropping strategy, we find $I_{AB}^{+} = I_{AB}^{\times} \equiv 1 - H(\frac{1-\mathcal{V}}{2})$ and $I_{AE}^{+} = I_{AE}^{\times} \equiv 1 - H(\frac{1-\sqrt{1-\mathcal{V}^2}}{2})$ because Bob's and Eve's information gains are independent of the basis Alice chose. We thus find that the symmetric operation provides a method for simultaneously measuring two complementary observables, P_{+} and $P_{\times}$, even when Bob observes P_{+}. In this case, the outcome for Eve gives the information $I_{AE} = I(\rho; P_{\times})$ and that for Bob gives $I_{AB} = I(\rho; P_{+})$. When we also take into account the fact that the sifted key involves only the data for which

Alice's and Bob's bases agree, the above arguments imply that Bob's average information gain on the sifted key is given by

$$I_{AB} = \frac{1}{2}\{I\left(\rho_{i\times}; P_{\times}\right) + I\left(\rho_{i+}; P_{+}\right)\}, \tag{2.11}$$

whereas Eve's information gain is given by

$$I_{AE} = \frac{1}{2}(I\left(\rho_{i\times}; P_{+}\right) + I\left(\rho_{i+}; P_{\times}\right)) \tag{2.12}$$

for the symmetric operation.

We can now see that the information exclusion principle leads to the inequality $I_{AB} + I_{AE} \leq 1$. Since the bases Alice and Bob used in the BB84 protocol are conjugate, $|\langle 0_\times | 0_+ \rangle| = |\langle 0_\times | 1_+ \rangle| = |\langle 1_\times | 0_+ \rangle| = |\langle 1_\times | 1_+ \rangle| = 1/\sqrt{2}$ holds, and it follows from the information exclusion principle that the inequalities

$$I\left(\rho_{i+}; P_{+}\right) + I\left(\rho_{i+}; P_{\times}\right) \leq 1 \tag{2.13}$$

$$I\left(\rho_{i\times}; P_{+}\right) + I\left(\rho_{i\times}; P_{\times}\right) \leq 1 \tag{2.14}$$

should hold. Equations (2.11) and (2.12) and inequalities (2.13) and (2.14) imply that $I_{AB}+I_{AE} \leq 1$. Since the optimal strategy is the best Eve can do, the inequality $I_{AB}+I_{AE} \leq 1$ holds for any strategy Eve may try. We therefore conclude that the bound on the sum of Bob's and Eve's information $I_{AB} + I_{AE} \leq 1$ is a direct consequence of the information exclusion principle.

It is helpful for later discussion to point out that the information exclusion principle is directly related to the fundamental equation between fringe visibility $\mathcal{V}$ and which-way information (path distinguishability) $\mathcal{D}_{opt}$ in one-particle interferometry [39–44]. To demonstrate this point, we note that the identities $|0_\times\rangle\langle 0_\times| + |1_\times\rangle\langle 1_\times| = |0_+\rangle\langle 0_+| + |1_+\rangle\langle 1_+| \equiv I$, $|0_\times\rangle\langle 1_\times| + |1_\times\rangle\langle 0_\times| \equiv |0_+\rangle\langle 0_+| - |1_+\rangle\langle 1_+|$, and $|0_+\rangle\langle 1_+| + |1_+\rangle\langle 0_+| \equiv |0_\times\rangle\langle 0_\times| - |1_\times\rangle\langle 1_\times|$ hold for a two-level system. We then find that

Bob's marginal density matrices ρ^B_{0x} or ρ^B_{1x} can be rewritten in terms of the complementary basis as

$$\rho^B_{0\times} = \frac{1}{2}\left\{|0_+\rangle\langle 0_+| + |1_+\rangle\langle 1_+| + \mathcal{V}\left(|0_+\rangle\langle 1_+| + |1_+\rangle\langle 0_+|\right)\right\}, \tag{2.15}$$

$$\rho^B_{1\times} = \frac{1}{2}\left\{|0_+\rangle\langle 0_+| + |1_+\rangle\langle 1_+| - \mathcal{V}\left(|0_+\rangle\langle 1_+| + |1_+\rangle\langle 0_+|\right)\right\}, \tag{2.16}$$

$$\rho^B_{0+} = \frac{1}{2}\left\{|0_\times\rangle\langle 0_\times| + |1_\times\rangle\langle 1_\times| + \mathcal{V}\left(|0_\times\rangle\langle 1_\times| + |1_\times\rangle\langle 0_\times|\right)\right\}, \tag{2.17}$$

$$\rho^B_{1+} = \frac{1}{2}\left\{|0_\times\rangle\langle 0_\times| + |1_\times\rangle\langle 1_\times| - \mathcal{V}\left(|0_\times\rangle\langle 1_\times| + |1_\times\rangle\langle 0_\times|\right)\right\}. \tag{2.18}$$

These equations are isomorphic to the equations describing one-particle interferometry where $\mathcal{V}$ gives the fringe visibility and $\mathcal{D}_{opt} = \sqrt{1-\mathcal{V}^2}$ gives the maximal which-way information (path distinguishability), satisfying $\mathcal{D}^2 + \mathcal{V}^2 \leq \mathcal{D}^2_{opt} + \mathcal{V}^2 = 1$ [39,40]. Note that the initial states that Alice transmitted are given by setting $\mathcal{V} = 1$ in these equations. This implies that the noise introduced by eavesdropping reduces the coherence (the off-diagonal terms) of the initial states, and that Bob's bit error probability $Q^B_e = \frac{1-\mathcal{V}}{2}$ due to eavesdropping can also be detected by observing the fringe visibility $\mathcal{V}$ in some kinds of interferometry.

III. BB84 PROTOCOL USING TWO COHERENT STATES AND THEIR SUPERPOSITION

The information exclusion principle ensures there is an upper bound on the eavesdropper's information gain and enables us to estimate this upper bound from that of the legitimate user. The requirement for this principle to be valid, on the other hand, does not mean that a single-photon state must be used as a signal carrier, but that the conjugate bases must belong to the same Hilbert space. In other words, we must choose *the conjugate observables that operate within the same signal-state space.* This requirement is satisfied when the polarization space of a single photon is used to encode information. For this purpose, we require a single-photon source, which has not yet been realized. To overcome this difficulty, a self-checking source, the validity of which can be self-checked, has been devised by Mayers et al. [45,46] Alternatively, many experimental implementations of BB84 have used weak coherent pulses (WCP), rather than single photons; in these implementations, four equiprobable states given by

$$\begin{aligned} &\left|0_0^{wcp}\right\rangle = \left|\alpha\right\rangle_1 \left|\alpha\right\rangle_2, \quad \left|1_0^{wcp}\right\rangle = \left|\alpha\right\rangle_1 \left|-\alpha\right\rangle_2 \\ &\left|0_{\pi/2}^{wcp}\right\rangle = \left|\alpha\right\rangle_1 \left|i\alpha\right\rangle_2, \quad \left|1_{\pi/2}^{wcp}\right\rangle = \left|\alpha\right\rangle_1 \left|-i\alpha\right\rangle_2 \end{aligned} \tag{3.1}$$

were used. [47–52] Note that $|\pm i\alpha\rangle = \left(e^{\mp\frac{\pi}{4}}/\sqrt{2}\right)[|\alpha\rangle \mp i\,|-\alpha\rangle] + O(\alpha^2)$. Therefore, if we consider only the first order in α (i.e., consider only a single-photon component), the four states would behave much like the ideal BB84 states. However, if we consider higher orders in α, the two states in one basis $|i_0^{wcp}\rangle$ are no longer linear combinations of the two states in the other basis $\left|i_{\pi/2}^{wcp}\right\rangle$, and thus do not satisfy the above requirement [53]. As a result, this implementation is vulnerable to eavesdropping. When α is large, these states are four non-orthogonal states lying in a four-dimensional signal state space instead of two sets of two orthogonal states lying in the two-dimensional signal state space used in the original single-photon implementation. There are eavesdropping strategies that make use of the linear independence of the four states. Figure 2 illustrates the relevant subspace of the four states in the entire Hilbert space (the Fock space). Because of the linear independence of the states, there are non-overlapping subspaces in the four states. The states lying in this subspace can be perfectly distinguished from each other, and a skillful eavesdropper can make use of this flaw to obtain information about the key *without detection* [13–15,53]. For example, Reid has described a strategy that makes use of this flaw, called the conclusive-measurement attack, in which Eve can sometimes get full information by using an appropriate “positive operator-valued measure” (POVM) [18,27,32] that conclusively distinguishes such linearly independent states [15]. Such measurement yields no information about the state most of the time, but it sometimes identifies the state unambiguously. This is fatal in the presence of high channel losses between Alice and Bob because Eve can recreate the state near Bob and send it to him without loss by substituting a lossless channel whenever she is able to measure the signal state unambiguously (otherwise she forwards nothing to Bob).

Another strategy, called the generalized beamsplitter attack, that makes use of this flaw has been reported on by several authors [13,47,48,54]. Since the polarization and photon number are independent observables, there is no problem in principle in selecting a few pulses with two or more photons and separating them into two one-photon pulses without changing the polarization, for example, by means of quantum nondemolition measurement [56]. If the loss in the channel between Alice and Bob is large enough, Eve can resend the remaining photons to Bob without reducing the bit rate by substituting the lossless channel and suppressing the signal without causing errors. As a result, Eve can obtain information about the key seemingly without introducing errors in the transmission. Thus, a high transmission loss together with the multi-photon components of the signal states render the key distribution in all key-distribution schemes vulnerable, unless a strong reference pulse is used to protect against eavesdroppers who can suppress a signal without causing errors by sending a vacuum state to Bob [5]. This vulnerablity arises because that the states $|i_0^{wcp}\rangle$ and$\left|i_{\pi/2}^{wcp}\right\rangle$ are linearly dependent only if we consider a single-photon component. They are linearly independent if we consider the multi-photon components of the signal states [53]. Thus, the use of the four coherent states in Eqs. (3.1) with a large α is inappropriate for the BB84 protocol, and Alice and Bob must use dim coherent pulses each of which, on average, typically contain 0.1 photons.

Nevertheless, the multi-photon state can be used to implement the BB84 protocol without this vulnerability. The basic idea of this scheme is depicted in Fig. 3. Two nearly orthogonal coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ are used to carry the key and the superposition of these states $(|\alpha\rangle \pm |-\alpha\rangle)/\sqrt{2(1 \pm \kappa)}$ is used to prevent from eavesdropping, where κ is the overlap of the two coherent states $|\alpha\rangle$ and $|-\alpha\rangle$; i.e., $\kappa = |\langle 0_+|\, 0_+\rangle| = |\langle\alpha|-\alpha\rangle| = e^{-2|\alpha|^2}$. These states are the "Schrödinger's cat states" and are parity eigenstates that lie within the relevant two-dimensional signal subspace spanned by $\{|\alpha\rangle\,, |-\alpha\rangle\}$ in the Fock state [55,57,58]. These four states would therefore behave much like ideal BB84 states.

In the following, we describe the protocol and explain how eavesdropping is detected. Consider the following protocol.

1. Alice first chooses a subset of random positions within a sequence of data being transmitted.

2. She then transmits random bits encoded with a set of nearly orthogonal states $|0_+\rangle = |-\alpha\rangle$ and $|1_+\rangle = |\alpha\rangle$ for the chosen subset (the first subset) which provides a secret key.

3. She also transmits either $|0_\times\rangle = (|\alpha\rangle - |-\alpha\rangle)/\sqrt{2(1-\kappa)}$ or $|1_\times\rangle = (|\alpha\rangle + |-\alpha\rangle)/\sqrt{2(1+\kappa)}$ for the remaining subset (the second subset) which will be used only to detect eavesdropping.

4. Alice also transmits a local oscillator beam (LO) with its polarization rotated so as to be orthogonal to the signal beam on the same channel by mixing the beams on a polarizing beamsplitter. The mixed beams are then transmitted to Bob.

5. Bob uses a polarizing beamsplitter to separate the LO from the channel. The polarization of the LO is rotated by $\pi/2$ using a $\pi/2$ plate so as to match that of the signal. With this LO, Bob performs homodyne detection to measure the single field-quadrature $\hat{x} = \hat{x}_a \cos\theta - \hat{p}_a \sin\theta = (1/\sqrt{2})[e^{i\theta}\hat{a} + e^{-i\theta}\hat{a}^\dagger]$ of the signal when he receives it, where $\hat{x}_a = (1/\sqrt{2})[\hat{a} + \hat{a}^\dagger]$, $\hat{p}_a = (1/\sqrt{2}i)[\hat{a} - \hat{a}^\dagger]$, and θ is the sum of the phase of the signal field and that of the LO (which is Bob's controllable parameter). He randomly varies θ between 0 and $\pi/2$ by changing the LO phase with phase shifter A.

6. After transmission, Alice publicly announces the positions of the first and second data subsets. Alice and Bob then discard the part of the first subset of data for which Bob measured $\hat{p}_a$ ($\theta = \pi/2$) and the part of the second subset of data for which he measured $\hat{x}_a$ ($\theta = 0$). Bob can obtain the sifted key from the first subset of the remaining data.

In terms of the sifted key, the conditional probability distributions $p_{i+}(x_a)$ of Bob's output x when Alice transmits signal i obey the Gaussian distributions:

$$\begin{aligned} p_{0+}(x_a) &= Tr\, |0_+\rangle\, \langle 0_+|\, x_a\rangle\, \langle x_a| \\ &= \frac{1}{\pi^{1/2}} \exp\left[-\left(x_a - \langle\alpha\rangle\right)^2\right], \qquad (3.2) \\ p_{1+}(x_a) &= Tr\, |1_+\rangle\, \langle 1_+|\, x_a\rangle\, \langle x_a| \end{aligned}$$

$$= \frac{1}{\pi^{1/2}} \exp\left[- \left(x_a + \langle \alpha \rangle \right)^2 \right], \tag{3.3}$$

where $\langle \alpha \rangle = \sqrt{2}\, |\alpha|$. The standard strategy for Bob to correctly infer the state transmitted by Alice is to set the decision threshold at $x_a = 0$; i.e., he sets the bit value to 0 when he obtains $x_a \geq 0$ and to 1 when he obtains $x_a < 0$. Then, his average error probability has finite value $Q_e^B(\alpha) = \frac{1}{2}\,\mathrm{Erfc}\left[\sqrt{2}\,|\alpha|\right]$, where Erfc$[x]$ is the complementary error function defined by $\mathrm{Erfc}[x] \equiv \left(1/\sqrt{2\pi}\right) \int_x^\infty \exp\left[-\tau^2\right] d\tau$ [59]. This is because the two coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ are not orthogonal. Bob also checks the second subset of remaining data to detect possible eavesdropping. Provided that Alice transmits the $|1_\times\rangle$ state for the second subset, the associated conditional probability distribution $p_{1\times}(p_a)$ is

$$p_{1\times}(p_a) = Tr\, |1_\times\rangle \langle 1_\times |\, p_a\rangle \langle p_a| = \frac{1}{(1+\kappa)} \frac{1}{\pi^{1/2}} \exp\left[-p_a^2\right] \left\{1 + \sin\left[2 \langle \alpha \rangle p_a\right]\right\}. \tag{3.4}$$

Therefore, when Bob builds up the probability distribution $p_{1\times}(p_a)$ of getting outcome p_a upon measurement of $\hat{p}_a$, the distribution should have interference fringes with a period of $\pi / \langle \alpha \rangle$ in the absence of eavesdropping [55,60].

To eavesdrop, Eve can, in principle, use a symmetric strategy by applying a joint unitary operation similar to the one shown in Eqs. (2.2) and (2.3). It involves complex multi-photon interaction between the single-mode field of the signal states and the probe system, and a physical mechanism that would enable such an operation has been unknown. Even if such an operation is realized, we can safely conclude that our proposed scheme is as secure as the single-photon case as far as this strategy is concerned by an argument similar to the single-photon case. This conclusion is closely related to the fact that the quantum mechanical superposition of macroscopically distinguishable states is cannot be noninvasively measured [61,62], which is essentially a direct consequence of the quantum mechanical complementarity. Moreover, this scheme is secure against a conclusive-measurement attack because the two mutually conjugate sets $|i_+\rangle$ and $|i_\times\rangle$ are linearly dependent. In the rest of the paper, we thus consider only a strategy that can only be used for cryptographic schemes using multi-photon states, that is, a beamsplitter attack. We show that, unlike the WCP implementation, the intentional eavesdropping activity will be detected by the legitimate users, and explain how the eavesdropping is detected.

We consider the following scenario. Eve uses a beam splitter (BS) to sample part of the signal. She sends Bob the part of the signal transmitted through the BS and measures the reflected part to gain information about the signal. What we want to know is how much she can learn and how much she disturbs the signal state. For this purpose, it is sufficient to calculate Eve's error rate Q_e^E for this particular scheme. If we denote the signal mode defined by the quantum channel as a and an auxiliary mode introduced at the BS as b, the associated joint unitary operation of the BS on coherent state input is

$$\left|0_+\right\rangle_a \left|0\right\rangle_b \to U_{BS} \left|\alpha\right\rangle_a \left|0\right\rangle_b = \left|\sqrt{T}\alpha\right\rangle_a \left|-\sqrt{R}\alpha\right\rangle_b , \tag{3.5a}$$

$$\left|1_+\right\rangle_a \left|0\right\rangle_b \to U_{BS} \left|-\alpha\right\rangle_a \left|0\right\rangle_b = \left|-\sqrt{T}\alpha\right\rangle_a \left|\sqrt{R}\alpha\right\rangle_b , \tag{3.5b}$$

where $T = \sqrt{1-R^2}$ is the transmission coefficient of the BS [63]. On the other hand, the same unitary operation transforms the $\left|1_\times\right\rangle$ state as

$$\left|0_\times\right\rangle_a \left|0\right\rangle_b \to U_{BS} \frac{\left|\alpha\right\rangle_a + \left|-\alpha\right\rangle_a}{\sqrt{2(1+\kappa)}} \left|0\right\rangle_b = \frac{1}{\sqrt{2(1+\kappa)}} \left\{ \left|\sqrt{T}\alpha\right\rangle_a \left|-\sqrt{R}\alpha\right\rangle_b + \left|-\sqrt{T}\alpha\right\rangle_a \left|\sqrt{R}\alpha\right\rangle_b \right\} , \tag{3.6}$$

which represents the entangled states of modes a and b even though the BS is a linear device. Therefore, noise is inevitably introduced into the transmission of the $\left|1_\times\right\rangle$ state. The associated marginal density matrices, ρ_{i+}^B and $\rho_{1\times}^B$ for Bob and ρ_{i+}^E and $\rho_{1\times}^E$ for Eve after the beamsplitter are calculated as

$$\rho_{i+}^B = tr_E U_{BS} \rho_{i+}^a \otimes \left|0\right\rangle_b \left\langle 0\right| U_{BS}^{-1} = \left|\pm\sqrt{T}\alpha\right\rangle_a \left\langle \pm\sqrt{T}\alpha\right| , \tag{3.7}$$

$$\begin{aligned}\rho_{1\times}^B &= tr_E U_{BS} \rho_{1\times}^a \otimes \left|0\right\rangle_b \left\langle 0\right| U_{BS}^{-1} \\ &= \frac{1}{2(1+\kappa)} \left\{ \left|\sqrt{T}\alpha\right\rangle_a \left\langle \sqrt{T}\alpha\right| + \left|-\sqrt{T}\alpha\right\rangle_a \left\langle -\sqrt{T}\alpha\right| \right. \\ &\quad \left. + \mathcal{V}_B \left(\left|\sqrt{T}\alpha\right\rangle_a \left\langle -\sqrt{T}\alpha\right| + \left|-\sqrt{T}\alpha\right\rangle_a \left\langle \sqrt{T}\alpha\right| \right) \right\} ,\end{aligned} \tag{3.8}$$

$$\rho_{i+}^E = tr_B U_{BS} \rho_{i+}^a \otimes \left|0\right\rangle_b \left\langle 0\right| U_{BS}^{-1} = \left|\mp\sqrt{R}\alpha\right\rangle_a \left\langle \mp\sqrt{R}\alpha\right| , \tag{3.9}$$

$$\begin{aligned}
\rho_{1\times}^{E} &= tr_B U_{BS} \rho_{1\times}^{a} \otimes |0\rangle_b \langle 0| U_{BS}^{-1} \\
&= \frac{1}{2(1+\kappa)} \left\{ \left|\sqrt{R}\alpha\right\rangle_a \left\langle \sqrt{R}\alpha\right| + \left|-\sqrt{R}\alpha\right\rangle_a \left\langle -\sqrt{R}\alpha\right| \right. \\
&\quad \left. + \mathcal{V}_E \left(\left|\sqrt{R}\alpha\right\rangle_a \left\langle -\sqrt{R}\alpha\right| + \left|-\sqrt{R}\alpha\right\rangle_a \left\langle \sqrt{R}\alpha\right| \right) \right\}, \qquad (3.10)
\end{aligned}$$

where $\rho_{i+}^{a} = |i_+\rangle_a \langle i_+| = |\pm\alpha\rangle_a \langle \pm\alpha|$, $\rho_{1\times}^{a} = |1_\times\rangle_a \langle 1_\times|$, $\mathcal{V}_B = \left|\left\langle \sqrt{R}\alpha\right| - \sqrt{R}\alpha\rangle\right| = e^{-2R|\alpha|^2}$, $\mathcal{V}_E = \left|\left\langle \sqrt{T}\alpha\right| - \sqrt{T}\alpha\rangle\right| = e^{-2T|\alpha|^2}$ (note that $\mathcal{V}_B\mathcal{V}_E = \kappa$), and the upper sign (resp. lower sign) corrsponds to $i = 1$ (resp. $i = 0$). Provided that Eve uses an optimum decision strategy that results in the smallest possible error when distinguishing two non-orthogonal coherent states $\left|\sqrt{R}\alpha\right\rangle_a$ and $\left|-\sqrt{R}\alpha\right\rangle_a$, her error rate Q_e^E is given by

$$Q_e^E = \frac{1 - \sqrt{1 - \mathcal{V}_B^2}}{2}. \qquad (3.11)$$

Such an optimum decision strategy is, in principle, realizable [64–66].

What Alice and Bob want to do is to evaluate Q_e^E or Eve's average information gain $I_{AE} = 1 - H(Q_e^E)$ as a function of the disturbance observable in the signal that Bob recorded. When we note that Eq. (3.8) is formally isomorphic to Eq. (2.16), we find that the most appropriate measure of the disturbance is the fringe visibility observable in the probability distribution $p_{1\times}(p_a)$. From Eq. (3.8), $p_{1\times}(p_a)$ in the presence of eavesdropping can be easily calculated as

$$p_{1\times}(p_a) = Tr \rho_{1\times}^{B} |p_a\rangle \langle p_a| = \frac{1}{(1+\kappa)} \frac{1}{\pi^{1/2}} \exp\left[-p_a^2\right] \left\{1 + \mathcal{V}_B \sin\left[2\sqrt{T}\langle\alpha\rangle p_a\right]\right\}. \qquad (3.12)$$

The fringe visibility is therefore given by $\mathcal{V}_B$. Figure 4 shows Eve's average information gain $I_{AE} = 1 - H(Q_e^E)$ calculated from Eq. (3.11) as a function of the fringe visibility $\mathcal{V}_B = e^{-2(1-T)|\alpha|^2}$ by changing T as a freely controllable parameter when the average photon number is assumed to be $|\alpha|^2 = 2$. This figure clearly indicates that the amount of information leaked to an eavesdropper can be estimated from the visibility of the interference fringe in the probability distribution $p_{1\times}(p_a)$ of getting outcome p_a upon homodyne-detection measurement of $\hat{p}_a$. This scheme is thus secure even against the beamsplitter attack even though the multi-photon states are used as a signal carrier. Figure 4 also plots Bob's information gain $I_{AB} = 1 - H(Q_e^B)$ on the sifted key under the assumption that he performed homodyne detection and the standard decision strategy stated above. In contrast to the single-photon implementation, where $I_{AB} = 1$ for this type of asymmetric attack, Bob's information vanishes in the low fringe-visibility region. This is because the intensity of the signal going to Bob falls to zero.

Figure 4 indicates that to learn about Alice's state with some degree of accuracy, Bob's visibility $\mathcal{V}_B$ must not be too large, which implies that the reflection coefficient $1 - T$ must not be too small. The requirements for a large information gain and little disturbance are thus incompatible. A large information gain requires a small transmission coefficient, while a small disturbance requires a transmission coefficient close to one, and there is no overlap in the permitted ranges. Therefore, with our QKD scheme, Eve cannot use this strategy and diverts enough light to gain any useful information without producing a detectable disturbance. This confirms the impossiblity of noninvasive measurement of the quantum-mechanical superposition of macroscopically distinguishable states. The problem for Eve is the vacuum noise from the vacant port of the BS. If she samples only a small part of the signal, to minimize the disturbance, the noise from the vacuum state obscures the information carried by the signal state [14].

This QKD scheme has advantages over the conventional schemes that use a single photon or a weak coherent pulse. First, in comparison with single-photon scheme, this scheme involves only quadrature phase measurements, which can be done more efficiently than photon counting. Second, in comparison with the WCP scheme, this scheme can use a more intense pulse, which can improve the transmission efficiency. However, the cat state is so fragile that the loss of the single photon may easily destroy the interference fringe observed in the probability distribution $p_{1\times}(p_a)$. Moreover, the decoherence rate of the cat state is proportional to the distance between the two distinguishable coherent states; i.e., it is proportional to $\sqrt{1-\kappa^2} \sim |\alpha|$ [55,60]. A cat state with a very large average photon number $|\alpha|^2$ is thus undesirable. On the other hand, there is a lower bound on the average photon number $|\alpha|^2$ that enebles use of the cat state to detect eavesdropping. To evaluate the fringe visibility, there should be at least one oscillation in the distribution $p_{1\times}(p_a)$ within the Gaussian contour $\exp[-p_a^2]$. This requirement should impose the inequality $\Delta p_a = \pi/(2\sqrt{2T}\,|\alpha|) < 2\sqrt{\ln 2}$. Thus, at least, $|\alpha| > \pi/(4\sqrt{2\ln 2}) \sim 0.67$ is required. In conclusion, we think a cat state with an average photon number of the order of unity is appropriate for our scheme. In this sense, what is needed is not a "macroscopic" quantum superposition but a "mesoscopic" quantum superposition which should be easier to create.

In terms of current feasibility, our scheme is limited by its susceptibility to channel loss, which is a problem because it also destroys the fringes in the distribution $p_{1\times}(p_a)$. In contrast, the channel loss is simply discarded in the WCP scheme, but this discarding also makes the WCP scheme vulnerabe because an eavesdropper can use it while substituting a superior channel to escape detection. It is this extreme sensitivity of the nonclassical field state (like the cat state) to the environment, though, that enables us to detect eavesdropping. The current feasibility of our scheme is also limited by the difficulty of preparing the cat state with today's technology. However, a development of a quantum gate will help us to obtain the cat state through a swapping operation [67] between a coherent state and a more easily created superposition state of a single quanta [57,68].

IV. CONCLUSION

We have developped a quantum key-distribution scheme that uses two nearly orthogonal coherent states to carry the key, and the superposition of these states to protect the communication channel from eavesdropping. This scheme is secure against conclusive-measurement attack and beamsplitter attack even in the presence of loss; these types of attack are believed to be a potential risk when a multi-photon state is used as a quantum carrier. We expect this scheme to be as secure as the single-photon scheme and secure against any optimal eavesdropping strategy. The disappearance of interference fringes in the homodyne detection used to decode the key clearly indicates eavesdropping activity, and the amount of information leaked to an eavesdropper can be estimated from the visibility of the interference fringes which is measurable from the homodyne detection.

ACKNOWLEDGMENTS

We thank Dominic Mayers for his helpful discussions.

REFERENCES

[1] S. Wiesner, Sigact News, **15**, 78 (1983).

[2] C. H. Bennett, G. Brassard, *Proc. of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, December 1984, pp. 175–179.

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[6] C. H. Bennet, G. Brassard, C. Crépeau, and M. Maurer: Generalized privacy amplification. IEEE trans. Inf. Theo. **41**, 1915 (1995).

[7] C. H. Bennet, F. Bessette, G. Brassard, L Salvail, and J. Smolin: J. Cryptology **5**, 2 (1992).

[8] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).

[9] D. Mayers, e-print quant-ph/9802025.

[10] B. Huttner and A. K. Ekart, J. Mod. Opt. **41**, 2455-2466 (1994).

[11] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).

[12] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).

[13] T. Ralph, e-print quant-ph/9907073.

[14] M. Hillery, e-print quant-ph/9909006.

[15] M. D. Reid, e-print quant-ph/9909030.

[16] M. J. Hall, Phys. Rev. Lett. **74**, 3307 (1995).

[17] K. Kraus, Phys. Rev. **D 35**, 3070 (1987).

[18] A. Peres, *Quantum theory: concepts and methods* (Kluwer, Dordrecht, 1998), Chap. 9.

[19] C. M. Caves and P. D. Drummond, Rev. Mod. Phys. **66**, 481 (1994).

[20] C. A. Fuchs, N. Gisin, R. B. Griffiths, C-S. Niu, and A. Peres, Phys. Rev. **A 56**, 1163 (1997).

[21] V. Buzěk and M. Hillery, Phys. Rev. **A 54**, 1844 (1996).

[22] D. Bruß, D. P. Divicenzo, A. Ekart, D. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. **A 57**, 2368 (1998).

[23] N. Gisin and B. Huttner, Phys. Lett. **A 228**, 13-21 (1997).

[24] J. I. Cirac and N. Gisin, Phys. Lett. **A 229**, 1-7 (1997).

[25] B. Schumacher, Phys. Rev. **A 54**, 2614 (1996).

[26] B. Schumacher and M. A. Nielsen, Phys. Rev. **A 54**, 2629 (1996).

[27] J. Preskill, *Quantum information and computation*, Lecture notes for physics 229 in CALTEC (1998).

[28] R. S. Kennedy, Mass. Inst. Tech. Res. Lab. Electron. Quart. Prog. Rep. No. 110, 142 (1974).

[29] E. B. Davis, IEEE Trans. Inf. Theory **IT-24**, 596 (1978).

[30] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. **A 54**, 3783 (1996).

[31] L. B. Levitin, in Workshop on Physics and Computation: Phys. Comp '92, edited by D. Matzke (IEEE Computer Society Press, Los Alamitos, CA, 1993).

[32] C. W. Helstrom, *Quantum detection and estimation theory* (Academic, New York, 1976).

[33] L. B. Levitin, in *Information Complexity and Control in Quantum Physics*, edited by

A. Blaquiere, S. Diner, and G. Lochak (Springer, Berlin, 1987), p. 15.

[34] P. Busch, e-print quant-ph/9604014.

[35] G. Jaeger and A. Shimony, Phys. Lett. **A 128**, 19 (1995).

[36] A. D. Wyner, Bell Syst. Tech. J. **54**, 1355 (1975).

[37] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[38] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 722 (1992).

[39] B-G. Englert, Phys. Rev. Lett. **77**, 2154 (1996).

[40] L. Mandel, Opt. Lett. **16**, 1882 (1991).

[41] S. Dürr, T. Nonn, and G. Rempe, Phys. Rev. Lett. **81**, 5705 (1998).

[42] G. Jaeger, M. A. Horne, and A. Shimony, Phys. Rev. **A 48**, 1023 (1993).

[43] G. Jaeger, A. Shimony, and L. Vaidman, Phys. Rev. **A 51**, 54 (1995).

[44] W. K. Wootters and W. H. Zurek, Phys. Rev. **D 19**, 473 (1979).

[45] D. Mayers and Andrew Yao, in *Proceedings of 39th Annual Symposium on Foundations of Computer Science*, 503 (1998), e-print quant-ph/9809039.

[46] D. Mayers, Y. Kohno, Y. Nambu, and A. Tomita, to be published in Phys. Rev. Lett.

[47] H. Yuen, Quantum Semiclass. Opt. **8**, 939-949 (1996).

[48] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. **A 51**, 1863 (1995).

[49] Y. Mu, J. Seberry, and Y. Zheng, Opt. Commun. **123**, 344 (1996).

[50] P. D. Townsend, J. G. Rality, and P. R. Tapster, Electron. Lett. **29**, 634 (1993).

[51] P. D. Townsend, J. G. Rality, and P. R. Tapster, Electron. Lett. **29**, 1291 (1993).

[52] P. D. Townsend, Electron. Lett. **30**, 809 (1994).

[53] G. Brassard, Tal Mor, and B. C. Sanders, e-print quant-ph/9906074.

[54] H. K. Lo and H. F. Chu, Science **283**, 2050 (1999); with supplementary material available at http://www.sciencemag.org/feature/data/984035.shl.

[55] B. Yurke and D. Stoler, Phys. Rev. Lett. **57**, 13 (1986).

[56] Y. Yamamoto, in *Encyclopedia of Applied Physics, vol. 15*, pp. 307-337 (VCH Publishers, 1996).

[57] P. T. Cochrane, G. J. Milburn, and W. J. Munro, Phys. Rev. **A 59**, 2631 (1999).

[58] V. Buzek and P. L. Knight, *Progress in Optics XXXIV*, edited by E. Wolf (North-Holland, Amsterdam, 1995).

[59] M. Osaki, M. Ban, and O. Hirota, Phys. Rev. **A 54**, 1691 (1996).

[60] D. F. Walls and G. J. Milburn, Phys. Rev. **A 31**, 2403 (1985).

[61] L. E. Ballentine, Phys. Rev. Lett. **59**, 1493 (1987).

[62] A. Peres, Phys. Rev. Lett. **61**, 2019 (1988).

[63] S. M. Barnett and P. M. Radmore, *Methods in theoretical quantum optics* (Clarendon, Oxford, 1997).

[64] M. Sasaki and O. Hirota, Phys. Lett. **A 210**, 21 (1996).

[65] M. Sasaki, T. S. Usuda, O. Hirota, and A. S. Holevo, Phys. Rev. **A 53**, 1273 (1996).

[66] M. Sasaki and O. Hirota, Phys. Rev. **A 54**, 2728 (1996).

[67] Y. Aharonov and L. Vaidman, e-print quant-ph/9909072.

[68] C. C. Gerry, Phys. Rev. **A 59**, 4095 (1999).

FIGURES

FIG. 1. Upper plot: Bob's information gain I_{AB}, Eve's information gain I_{AE} and their sum $I_{AB} + I_{AE}$ are plotted against Bob's error probability Q_e^B when Eve applys an optimum eavesdropping strategy. Lower plot: measures of information gained by Bob (G^B) and by Eve (G^E) are plotted.

FIG. 2. The relevant subspace of the four weak coherent states in the entire Hilbert space (the Fock state). The parts of the four circles that do not overlap indicate the linear independence of the states.

FIG. 3. The basic idea of the proposed QKD scheme. Alice and Bob use two nearly orthogonal coherent states to carry the key and the superposition of these states (cat states) to protect from eavesdropping. Eavesdropping is detected from the disappearance of the interferential fringes in the distribution of the outcome when a certain quadrature component is measured by the homodyne detection.

FIG. 4. Eve's average information gain $I_{AE} = 1 - H(Q_e^E)$ as a function of the fringe visibility $\kappa_B = e^{-2(1-T)|\alpha|^2}$ in the probability distribution $p_{1\times}(p_a)$ recorded by Bob. The average photon number is assumed to be $|\alpha|^2 = 2$.